

IN THE ABSTRACT:

Please replace the Abstract of the Invention with the following new Abstract. A clean copy of the Abstract is attached.

ABSTRACT OF THE ~~DISCLOSURE~~INVENTION

The encryption device includes a random number generator ~~means~~ for generating a random number; and a first selector for selecting one of q fixed values in response to the random number, a second selector for selecting one set of q sets of fixed ~~table~~S-box tables in response to the random number. An XOR ~~means~~ XORs an input with an XOR of a key with the fixed value. ~~Nonlinear~~ A nonlinear transform ~~means~~ nonlinearly transforms an input nonlinearly in accordance with the selected set of fixed ~~table~~S-box tables. Another encryption device includes a plurality of encrypting units coupled in parallel, and a selector for selecting one of the plurality of encrypting units in response to the random number. The masking with the fixed values improves ~~of~~ the processing speed and reduces the required RAM area.